Math 357
Expositional homework 06

Assigned: 2024–03–29 (F)
Due: 2024–04–12 (F)

The goal of this homework is to strengthen our understanding of field theory, through proof and example.

Proofs

(a) Prove Proposition 13.12:[1] Let $K : K_0$ be a field extension, and let $\alpha \in K$. Then α is algebraic over K_0 if and only if $[K_0(\alpha) : K_0] < \infty$.

(b) Prove Theorem 13.25[2] on the existence of splitting fields: Let K_0 be a field, and let $f \in K_0[t]$. Then there exists an extension field $K : K_0$ such that f splits completely in $K[t]$.

(c) Let $K : K_0$ be a field extension such that $[K : K_0] < \infty$. Prove that $K : K_0$ is normal if and only if for all irreducible polynomials $f \in K_0[t]$, if there exists an $\alpha \in K$ such that $f(\alpha) = 0$, then f splits completely in $K[t]$.[3] (One may take this as the definition of a normal field extension, in which case one can prove the definition we gave in class as a proposition.)

(d) Let K_0 be a field, and let $f_1, f_2 \in K_0[t]$. Prove that the formal derivative D_t of a polynomial in $K_0[t]$ satisfies the following relations (as does the derivative operator from calculus):[4]

$$D_t(f_1 + f_2) = D_t f_1 + D_t f_2 \qquad D_t(f_1 f_2) = (D_t f_1) \cdot f_2 + f_1 \cdot (D_t f_2)$$

Examples

(e) Determine the degree over $\mathbf{Q}$ of $2 + \sqrt{3}$ and $1 + \sqrt[3]{2} + \sqrt[3]{4}$.[5]

(f) Let $K : K_0$ be a field extension of finite degree n, and let $\alpha \in K$.[6]

[1] See DF3e, p 521.

[2] See DF3e, p 536. If you are up for it, then you can also prove that any two splitting fields for f are isomorphic; see Corollary 13.28, p 542. This will take a little work, but the theory and proof are both accessible and rewarding.

[3] See DF3e, Exercise 13.4.5, p 545.

[4] See DF3e, Exercise 13.5.1, p 551.

[5] See DF3e, Exercise 13.2.4, p 530.

[6] See DF3e, Exercises 13.2.19(a) and 20, p 531.

(i) Prove that the map

$$\begin{aligned} T_\alpha : K &\to K \\ \beta &\mapsto \alpha\beta \end{aligned}$$

which is (left) multiplication by α, is a K_0-linear transformation of K.

Let $n \in \mathbf{Z}_{>0}$, let M be an $n \times n$ matrix, let I be the $n \times n$ identity matrix, and let t be an indeterminate. The **characteristic polynomial** of M is $\det(tI - M) = (-1)^n \det(M - tI)$.

(ii) Let $\mathcal{B}$ be a K_0-basis of K, and let $M_{\mathcal{B}}(T_\alpha)$ be the matrix of T_α with respect to $\mathcal{B}$. Prove that α is a zero of the characteristic polynomial of $M_{\mathcal{B}}(T_\alpha)$.

(iii) Use this technique to find monic polynomials in $\mathbf{Q}[t]$ of degree 3 satisfied by $\sqrt[3]{2}$ and by $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

(g) Let $p \in \mathbf{Z}_{>0}$ be prime, let $\mathbf{F}_p = \mathbf{Z}/(p)$ (a finite field of order p), let $a \in \mathbf{F}_p$ be nonzero, and let $f = t^p - t + a \in \mathbf{F}_p[t]$. Prove that f is irreducible in $\mathbf{F}_p[t]$ and separable.[7]

Exercise (a)

See DF3e, pp 521–2.

Exercise (b)

For existence, see DF3e, p 536. For uniqueness (which we were not required to prove on this homework), see DF3e, pp 541–2.

Exercise (c)

($\Rightarrow$) Let $K : K_0$ be normal. Then by definition, there exists a set $S \subseteq K_0[t]$ such that K is a splitting field of S. By hypothesis, $[K : K_0] < \infty$, so there exists a finite subset $S' \subseteq S$ such that K is a splitting field of S'. Let $f_0 = \prod_{g \in S'} g$. (Note that this construction uses that S' is finite.)

Let $f \in K_0[t]$ such that there exists an $\alpha \in K$ such that $f(\alpha) = 0_K$. Let β be a zero of f, potentially in some extension field over K. (For example, view $f \in K[t]$, let $\tilde{K}_f$ be a splitting field for f over K, and take $\beta \in \tilde{K}_f$.) By Theorem 13.8, there exists an isomorphism $\sigma_0 : K_0(\alpha) \to K_0(\beta)$ such that $\sigma_0(\alpha) = \beta$ and $\sigma_0|_{K_0} = \mathrm{id}_{K_0}$. Note that $K(\alpha)$ is a splitting field of f_0 over $K_0(\alpha)$, and $K(\beta)$ is a splitting field of f_0 over $K_0(\beta)$. Thus by Theorem 13.27, σ_0 extends to an isomorphism $\sigma : K(\alpha) \to K(\beta)$ such that $\sigma|_{K_0(\alpha)} = \sigma_0$. By hypothesis, $\alpha \in K$, so $K(\alpha) = K$. We conclude that $K(\beta) \cong K(\alpha) = K$, so $\beta \in K$ as well.

($\Leftarrow$) By Theorem 13.17, $[K : K_0] < \infty$ if and only if K is generated by a finite number, say n, of elements $\alpha_i \in K$, each of which is algebraic over K_0. Because α_i is algebraic over K_0, each α_i has a (unique) minimal polynomial $m_{\alpha_i, K_0} \in K_0[t]$, which by definition is irreducible. By definition, each m_{α_i, K_0} has a zero in K, namely α_i; so by hypothesis, each m_{α_i, K_0} splits completely in K.

Let $f_0 = \prod_{i=1}^{n} m_{\alpha_i, K_0}$. (Again, note that this construction uses that the indexing set of the product is finite.) Our argument in the preceding paragraph shows that f splits completely in K, and that K is generated by the zeros of f. Thus $K : K_0$ is normal (take $S = \{f_0\}$).

[7] See DF3e, Exercise 13.5.5, p 551.

Exercise (d)

This is a straightforward if tedious bookkeeping exercise.

Let $n_i = \deg f_i$, let $n = \max(n_1, n_2)$, let $N = n_1 + n_2$, and let

$$f_i = \sum_{j=0}^{n_i} a_{i,j} t^j \qquad \text{so} \qquad D_t f_i = \sum_{j=1}^{n_i} j \cdot a_{i,j} t^{j-1}$$

Let us adopt the convention that if the index $j > n_i$, then $a_{i,j} = 0$. Then

$$\begin{aligned}
D_t(f_1 + f_2) &= D_t \left(\sum_{j=0}^{n} (a_{1,j} + a_{2,j}) t^j \right) && \text{by definition of } + \text{ in a polynomial ring} \\
&= \sum_{j=1}^{n} j \cdot (a_{1,j} + a_{2,j}) t^{j-1} && \text{by definition of formal derivative} \\
&= \sum_{j=1}^{n} j \cdot a_{1,j} t^{j-1} + \sum_{j=1}^{n} j \cdot a_{2,j} t^{j-1} && \text{by field axioms} \\
&= D_t f_1 + D_t f_2 && \text{by definition of formal derivative}
\end{aligned}$$

Similarly,

$$\begin{aligned}
D_t(f_1 f_2) &= D_t \left(\sum_{j=0}^{N} \sum_{k=0}^{j} a_{1,k} a_{2,j-k} t^j \right) \\
&= \sum_{j=1}^{N} \sum_{k=0}^{j} j \cdot a_{1,k} a_{2,j-k} t^{j-1} \\
&= \sum_{j=1}^{N} \sum_{k=0}^{j} (k + j - k) \cdot a_{1,k} a_{2,j-k} t^{j-1} \\
&= \sum_{j=1}^{N} \sum_{k=0}^{j} k \cdot a_{1,k} a_{2,j-k} t^{j-1} + \sum_{j=1}^{N} \sum_{k=0}^{j} (j - k) \cdot a_{1,k} a_{2,j-k} t^{j-1} \\
&= D_t f_1 \cdot f_2 + f_1 \cdot D_t f_2
\end{aligned}$$

Exercise (e)

Let $\alpha = 2 + \sqrt{3}$. Then

$$\alpha - 2 = \sqrt{3} \qquad \Rightarrow \qquad (\alpha - 2)^2 = 3 \qquad \Leftrightarrow \qquad \alpha^2 - 4\alpha + 1 = 0$$

so α is a zero of the polynomial

$$f = t^2 - 4t + 1$$

Note that f is irreducible (why?[8]) and monic, so it is the minimal polynomial of α over $\mathbf{Q}$. Hence

$$\deg_{\mathbf{Q}} \alpha = \deg m_{\alpha,\mathbf{Q}} = \deg f = 2$$

[8]One can see that f is irreducible in various ways. One way is to reduce the coefficients mod 2 and show that the image of f has no zeros in $\mathbf{Z}/(2)$. Another way is to apply the rational zeros test to f directly.

Now let $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. Then

$$(\alpha-1)^3 = (\sqrt[3]{2} + \sqrt[3]{2}^2)^3 = 2 + 3\sqrt[3]{2}^4 + 3\sqrt[3]{2}^5 + 4 = 6(1 + \sqrt[3]{2} + \sqrt[3]{2}^2) = 6\alpha \quad \Leftrightarrow \quad (\alpha-1)^3 - 6\alpha = 0$$

so α is a zero of the polynomial

$$f = t^3 - 3t^2 - 3t - 1$$

Note that f is irreducible (why?[9]) and monic, so it is the minimal polynomial of α over $\mathbf{Q}$. Hence

$$\deg_{\mathbf{Q}} \alpha = \deg m_{\alpha,\mathbf{Q}} = \deg f = 3$$

Exercise (f)

Part (i): Let $\beta_1, \beta_2 \in K$, and let $a \in K_0$. Then

$$\begin{aligned} T_\alpha(a\beta_1 + \beta_2) &= \alpha(a\beta_1 + \beta_2) && \text{by definition of } T_\alpha \\ &= a\alpha\beta_1 + \alpha\beta_2 && \text{by the axioms of a field} \\ &= aT_\alpha(\beta_1) + T_\alpha(\beta_2) && \text{by definition of } T_\alpha \end{aligned}$$

so T_α is K_0-linear.

Part (ii): Let M denote $M_{\mathcal{B}}(T_\alpha)$; let $p = \det(tI - M)$ denote the characteristic polynomial of M; and let id_K denote the identity map on K, so $I = M_{\mathcal{B}}(\mathrm{id}_K)$. The intuition is that the matrix $\alpha I - M$ that appears in the expression for $p(\alpha)$ represents the map $\alpha\,\mathrm{id}_K - T_\alpha$, and for all $\beta \in K$,

$$(\alpha\,\mathrm{id}_K - T_\alpha)(\beta) = \alpha\,\mathrm{id}_K(\beta) - T_\alpha(\beta) = \alpha\beta - \alpha\beta = 0$$

We may be tempted to apply a result from linear algebra[10] that says $\det(\alpha I - M) = 0$ if and only if α is an eigenvalue of the corresponding linear map. However, we must be careful to correctly apply any theory from linear algebra. In our current setting, we view K as a K_0-vector space. In particular, $\alpha \in K$ corresponds to a vector, not a scalar. As such, α cannot be an eigenvalue. As illustrated in our response to part (iii) below, the matrix $\alpha I - M$ is not the zero matrix if (and only if) $\alpha \notin K_0$. Instead, we could view the characteristic polynomial $p \in K_0[t]$ as being an element of $K[t]$, or we could view the $n \times n$ matrix $\alpha I - M$ as operating on K^n and find an eigenvector there with eigenvalue α.

Part (iii): Let

$$\alpha = \sqrt[3]{2} \qquad\qquad \beta = 1 + \sqrt[3]{2} + \sqrt[3]{4} = 1 + \alpha + \alpha^2$$

Note that $\alpha, \beta \in \mathbf{Q}(\alpha)$; and $m_{\alpha,\mathbf{Q}} = t^3 - 2$ is the minimal polynomial for α over $\mathbf{Q}$ (why?), so $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg m_{\alpha,\mathbf{Q}} = 3$. Therefore, one $\mathbf{Q}$-basis for $\mathbf{Q}(\alpha)$ is $\mathcal{B} = (1, \alpha, \alpha^2)$. We compute the matrix representations with respect to this basis for the multiplication by α (respectively, β) map to be

$$M_{\mathcal{B}}(T_\alpha) = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad\qquad M_{\mathcal{B}}(T_\beta) = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

[9] The same approaches we took for $\alpha = 2 + \sqrt{3}$ above also work here.

[10] See DF3e, Proposition 12.12, p 473.

From these, we compute the characteristic polynomials to be

$$p_{T_\alpha} = t^3 - 2 \qquad\qquad p_{T_\beta} = t^3 - 3t^2 - 3t - 1$$

By construction, the characteristic polynomial is monic; by part (ii), it has the given element (α or β) as a zero; and (for these particular polynomials) one can verify each is irreducible. We conclude that each is the minimal polynomial of its respective element over $\mathbf{Q}$. (In general, the minimal polynomial will be a factor, irreducible over the base field, of the characteristic polynomial.)

Exercise (g)

Let K_0 be a perfect field, and let $f \in K_0[t]$. We have seen that if f is irreducible, then f is separable.[11] In particular, finite fields (for example, $\mathbf{F}_p$) are perfect. Thus for this exercise, it suffices to prove that f is irreducible.[12]

Lemma. Let $K : \mathbf{F}_p$, and let $\alpha \in K$ such that $f(\alpha) = 0_K$. Then K contains n distinct zeros of f.

Proof of lemma. Note that $\operatorname{char} K = \operatorname{char} \mathbf{F}_p = p$.[13] By hypothesis,

$$0_K = f(\alpha) = \alpha^p - \alpha + a$$

Note that, for all $x, y \in K$,

$$(x+y)^p = x^p + \binom{p}{1} \cdot x^{p-1}y + \ldots + \binom{p}{p-1} \cdot xy^{p-1} + y^p = x^p + y^p$$

where for the final equality, we observe that for $1 \leqslant m \leqslant p-1$, $\binom{p}{m}$ is divisible by p in $\mathbf{Z}$; because $\operatorname{char} K = p$, all "middle" terms are zero in K. Using this, we compute

$$f(\alpha + 1_K) = (\alpha + 1_K)^p - (\alpha + 1_K) + a = \alpha^p + 1_K - \alpha - 1_K + a = \alpha^p - \alpha + a = f(\alpha) = 0$$

We conclude that if an extension field $K : \mathbf{F}_p$ contains one zero α of f, then it contains all n zeros of f. More precisely, these zeros are

$$\alpha, \alpha + 1_K, \ldots, \alpha + (p-1) \cdot 1_K$$

Because $\operatorname{char} K = p$, these zeros are distinct,[14] as desired.

Note that the lemma also shows, directly, that f is separable.

Corollary. f contains no zeros in $\mathbf{F}_p$.

Proof. Suppose for the sake of contradiction that there exists an $\alpha \in \mathbf{F}_p$ such that $f(\alpha) = 0$. Then the lemma implies that

$$f = \prod_{\beta \in \mathbf{F}_p} (t - \beta)$$

[11] See DF3e, p 549.

[12] That said, we can give a quick proof that f is separable using the formal derivative. Recall (see DF3e, Proposition 13.33, p 547.) that a polynomial f is separable if and only if $\gcd(f, D_t f) = 1$. Using that $\operatorname{char} \mathbf{F}_p = p$, we compute

$$D_t f = D_t(t^p - t + a) = (p \cdot 1_{\mathbf{F}_p})t^{p-1} - 1 + 0 = -1$$

Therefore $\gcd(f, D_t f) = 1$, so f is separable.

[13] This follows immediately in both the subfield ($\mathbf{F}_p \subseteq K$) and injective field homomorphism ($\mathbf{F}_p \to K$) view of a field extension $K : \mathbf{F}_p$.

[14] More precisely, suppose that there were $m, n \in \{0, \ldots, p-1\}$ such that $m \neq n$ and $\alpha + m \cdot 1_K = \alpha + n \cdot 1_K$ in K. Without loss of generality, assume $n > m$. Then $0 = (n-m) \cdot 1_K$ with $n - m < p$, contradicting $\operatorname{char} K = p$.

In particular, $a = f(0) = 0$, contradicting the hypothesis that $a \neq 0$.

We now use the lemma to show that f is irreducible (and hence separable). Let

$$f = \prod_{i=1}^{n} f_i$$

be a factorization of f into irreducible factors $f_i \in \mathbf{F}_p[t]$. Because f is monic, without loss of generality, we may assume that each f_i is monic.[15] We wish to show that $n = 1$.

Claim: The degree of each factor f_i of f is equal. To see this, let K be a splitting field for f over $\mathbf{F}_p$. For each $i \in \{1, \ldots, n\}$, let $\alpha_i \in K$ be a zero of f_i. Because each f_i is irreducible and monic, f_i is the minimal polynomial of α_i over $\mathbf{F}_p$, denote it $m_{\alpha_i, \mathbf{F}_p}$. Because α_i is a zero of f_i, it is also a zero of f. Hence by the lemma,

$$\alpha_i \in \{\alpha_1, \alpha_1 + 1_K, \ldots, \alpha_1 + (p-1) \cdot 1_K\} \subseteq K$$

That is, for each $i \in \{1, \ldots, n\}$, there exists a $m_i \in \{0, \ldots, p-1\} \subseteq \mathbf{Z}$ such that

$$\alpha_i = \alpha_1 + m_i \cdot 1_K$$

It follows that, for each $i \in \{1, \ldots, n\}$,

$$f_1(t - m_i \cdot 1_K)$$

is an irreducible, monic polynomial in $\mathbf{F}_p[t]$ with α_i as a zero. That is,

$$f_1(t - m_i \cdot 1_K) = m_{\alpha_i, \mathbf{F}_p}(t) = f_i(t)$$

so

$$\deg f_i(t) = \deg f_1(t - m_i \cdot 1_K) = \deg f_1(t)$$

proving the claim.

Let $d = \deg f_i$ denote the common degree of each (irreducible) factor f_i of f. Because $\mathbf{F}_p$ is a field (and hence an integral domain),

$$p = \deg f = \deg \prod_{i=1}^{n} f_i = \sum_{i=1}^{n} \deg f_i = nd$$

Because p is prime, $p \mid n$ or $p \mid d$. If $p \mid n$, then we must have $n = p$ and $d = 1$. However, $d = 1$ implies that each $\alpha_i \in \mathbf{F}_p$, contradicting the corollary above. Therefore we must have $n = 1$ and $d = p$. That is, f is irreducible in $\mathbf{F}_p[t]$, as desired.

[15] Because $\mathbf{F}_p$ is a field, by definition of polynomial multiplication, the product of the leading coefficients of all the f_i equals the leading coefficient of f, which is $1_{\mathbf{F}_p}$. Factoring out the leading coefficient from each f_i leaves each f_i monic, and the product of these leading coefficients equals $1_{\mathbf{F}_p}$ and hence does not change the product.